BUNDESREPUBLIK DEUTSCHLAND

Bescheinigung

Die Deutsche Telekom AG in Bonn/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Verfahren zur gesicherten Übertragung von Nachrichten"

am 20. Mai 1998 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig die Symbole H 04 K und H 04 L der Internationalen Patentklassifikation erhalten.

München, den 11. März 1999
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Aktenzeichen: 198 22 685.3

Wallner

A 9161
06 90
11/98

97TK 1505DEP

Verfahren zur gesicherten Übertragung von Nachrichten

Beschreibung

Die vorliegende Erfindung betrifft ein Verfahren zur gesicherten Übertragung von Nachrichten zwischen zumindest zwei Benutzern eines Telefonkommunikationsnetzes. Sie betrifft zudem ein Verschlüsselungssystem zur Durchführung dieses Verfahrens mit den zugehörigen technischen Einrichtungen.

Durch das Vordringen von Computern in nahezu alle Lebensbereiche und ihre zunehmende Vernetzung untereinander durch großräumige Telekommunikationsnetze ist der Strom des Datenverkehrs zwischen Rechnern unterschiedlichster Art enorm angestiegen. Viele der ausgetauschten Informationen sind vertraulich und sollen und/oder dürfen von unbefugten Dritten nicht mitgelesen werden können, so daß ein großer Bedarf an einer kryptographischen Absicherung dieses Datenverkehrs besteht. Einfache kryptographische Verfahren halten aber einer Kryptoanalyse mit Hilfe von Rechnern nicht stand, so daß ein großes Interesse an Verschlüsselungsverfahren besteht, die auch bei einem Einsatz von Rechnern unter Verwendung neuartiger Entschlüsselungsverfahren sicher sind.

Ähnliches gilt auch für einen Informationsaustausch beim Telefonieren oder Faxen, da durch einen Einsatz modernster Computertechnik in Verbindung mit automatischen Worterkennungstechniken sowohl im industriellen als auch im privaten Bereich praktisch jedes über öffentliche Übertragungskanäle gegangene Wort problemlos aufgezeichnet, später wieder gesucht und ausgewertet werden kann. Zumindest

Privatleute sind zur Zeit einem solchen Eingriff in ihre Intimssphäre praktisch noch schutzlos ausgeliefert, da es an einer hinreichenden Zugänglichkeit zu entsprechenden Verschlüsselungs- bzw. Entschlüsselungsverfahren und an entsprechenden Vorrichtungen zur Durchführung dieser Verfahren fehlt. Zudem können unbefugte Dritte bei einem Großteil der üblicherweise als relativ sicher geltenden bekannten Verschlüsselungsverfahren durch einen sehr großen Rechenaufwand und/oder neuartige Entschlüsselungsverfahren in den Besitz der ausgetauschten Informationen gelangen, was theoretisch auch durch eine staatliche Beschlagnahme des verwendeten Schlüssels möglich wäre.

Als absolut sicher bezüglich eines Entschlüsselungsversuchs durch Computereinsatz gelten zur Zeit lediglich Verschlüsselungsverfahren, bei denen vom Sender und Empfänger einer Nachricht jeweils der gleiche geheime zufällige Schlüssel benutzt wird, der solange wie die Nachricht selbst ist und nur einmal zur Verschlüsselung verwendet wird.

Die Aufgabe der vorliegenden Erfindung besteht daher in der Schaffung eines Verfahrens zur individuellen Erzeugung solch geheimer zufälliger Schlüssel und zum Austausch der erzeugten Schlüssel zwischen zumindest zwei Benutzern eines Telekommunikationsnetzes, um ausgetauschte Informationen, sei es durch Telefon, Fax oder PC, abhörsicher zu verschlüsseln. Die Aufgabe besteht zudem in der Schaffung eines Verschlüsselungssystems zur Durchführung dieses Verfahrens mit den zugehörigen technischen Einrichtungen.

Diese Aufgabe wird erfindungsgemäß durch das in Anspruch 1 angegebene Verfahren gelöst, wobei bevorzugte Ausführungsformen den Unteransprüchen 2 - 12 zu entnehmen sind.

Ein Verschlüsselungssystem zur Durchführung dieses

Verfahrens ist Anspruch 13 zu entnehmen, während in den Ansprüchen 14 bis 19 bevorzugte Ausführungsformen beansprucht werden.

Besondere Merkmale und Vorteile des erfindungsgemäßen Verschlüsselungsverfahrens, des erfindungsgemäßen Verschlüsselungssystems zur Durchführung dieses Verfahrens und der zugehörigen technischen Einrichtungen des Systems ergeben sich aus der nachfolgenden ausführlichen Beschreibung eines Ausführungsbeispiels, das in der zugehörigen Fig. 1 schematisch dargestellt ist.

Fig. 1 zeigt einen Schlüsselgenerator 10 zur Erzeugung eines zufälligen binären Schlüssels großer Länge, der im vorliegenden Ausführungsbeispiel mittels eines (nicht dargestellten) eingebauten optischen Zufallsgenerators mit Strahlteiler erzeugt wird, wie er beispielsweise der deutschen Patentanmeldung 196 41 754.6 zu entnehmen ist. Es kann jedoch auch ein Zufallsgenerator eingesetzt werden, bei dem die spontane Emission eines Photons in elektrisch oder optisch angeregter Materie oder der radioaktive Zerfall zur Schlüsselerzeugung verwendet wird. Denkbar ist auch die Verwendung eines physikalischen Rauschverfahrens oder eines sonstigen geeigneten physikalischen Verfahrens.

Der erzeugte Schlüssel wird nun ohne interne Speicherung durch eine (nicht dargestellte) eingebaute Schreibeinrichtung in dem Schlüsselgenerator 10 in zumindest zwei transportable Daten- oder Schlüsselträger 12 eingeschrieben und in dieser Form an einen Benuzter ausgegeben, wobei die Anzahl und eventuell auch die Art an ausgegebenen Datenträgern mittels einer (nicht dargestellten) Eingabetastatur durch den Benutzer frei wählbar ist. Als Datenträger 12 können hierbei, wie im vorliegenden Fall, CDs verwendet werden. Der Schlüssel kann beispielsweise jedoch auch auf Magnetbändern, auf geeigneten Halbleiterspeichern oder einer sonstigen geeigneten

transportablen Speichereinrichtung gespeichert und ausgegeben werden.

Der Schlüsselgenerator 10 ist öffentlich zugänglich, um möglichst breiten Bevölkerungskreisen eine kryptographische Absicherung ihrer Nachrichtenverbindungen zu ermöglichen. Es sollten daher möglichst viele Schlüsselgeneratoren 10 flächendeckend installiert werden, wobei darauf zu achten ist, daß die Stelle, die die aufgestellten Geräte 10 betreut, ein gewisses Vertrauen genießt, so wie dies beispielsweise bei der Post der Fall ist. Hierdurch ist die Gefahr einer Manipulation an den Geräten 10 und die Wahrscheinlichkeit, daß der Schlüssel auch an unbefugte Dritte gelangt und diese den Schlüssel einer bestimmten Person zuordnen können, relativ gering.

Die Anonymität bei der Schlüsselausgabe und damit die Sicherheit des Verschlüsselungsverfahrens wird noch dadurch erhöht, daß die Schlüsselgeneratoren 10 vorzugsweise durch Münzeinwurf oder durch Eingabe eines sonstigen Zahlungsmittels, wie z.B. eine entsprechende Magnetstreifenkarte, einfach aktivierbar sind, ohne daß sich der Benutzer hierfür ausweisen muß oder eventuell Daten der Magnetstreifenkarte gespeichert werden.

Es ist jedoch auch denkbar, daß größere Firmen etwa in Verbindung mit Standleitungen den gesamten Nachrichtenverkehr mit einem Empfänger, wie z.B. eine Tochterfirma oder eine Filiale, auf die angegebene Art und Weise verschlüsseln. In diesem Fall lohnt sich der Einsatz eines eigenen Schlüsselgenerators 10, der dann in der jeweiligen Firma installiert wird und dort den Firmenangehörigen oder aber auch nur einem begrenzten ausgewählten Personenkreis zugänglich ist, der sich zur Absicherung unter Umständen erst durch Eingeben einer persönlichen Geheimzahl ausweisen muß.

Angesichts des enormen Fortschritts der Technik ist es jedoch auch denkbar, daß Schlüsselgeneratoren 10 der genannten Art zukünftig so kostengünstig und kompakt herstellbar sind, daß sie auch für Privatpersonen erschwinglich werden und dann in großer Anzahl auch Eingang in Privathaushalte finden.

Die Anzahl der angegebenen Datenträger 12 ist über eine (nicht dargestellte) Eingabetastatur so wählbar, daß sie der Anzahl der miteinander kommunizierenden Benutzer entspricht. Bei einem Sender und einem Empfänger werden somit zwei Datenträger 12 ausgegeben, auf denen jeweils derselbe zufällige Schlüssel aufgezeichnet ist und von denen der Sender und der Emfpänger jeweils einen Datenträger 12 erhält. Die Übergabe der Datenträger 12 kann hierbei beispielsweise persönlich oder aber durch Zusendung per Post erfolgen. Ein sicherer Schlüsselaustausch kann auch unter Verwendung eines geeigneten Schlüsselverteilungssystems erfolgen, wie es bei Fachleuten auf diesem Gebiet beispielsweise unter der Bezeichnung "Quantenkryptographie" bekannt ist.

Zur Verschlüsselung einer Nachricht werden die Datenträger 12 von den Benutzern nun in Leseeinrichtungen 14 eingegeben, die den von den Benutzern, d.h. dem Sender einer Nachricht und dem zugehörigen Empfänger der Nachricht, zur Nachrichtenübermittlung verwendeten Telekommunikationssendeeinrichtungen 16, wie z.B. Telefone, Faxgeräte oder PCs, jeweils zugeordnet sind und zum Einlesen des jeweils verwendeten Schlüssels von den Datenträgern dienen.

Die ordnungsgemäße Eingabe des Schlüssels und die Übereinstimmung der von den Benutzern eingegebenen Schlüssel wird nun mit Hilfe von Logistikeinrichtungen 18 überprüft, die den zur Nachrichtenübermittlung verwendeten Telekommunikationssendeeinrichtungn 16 ebenfalls zugeordnet

sind und beim Aufbau einer Verbindung automatisch Kontakt miteinander aufnehmen.

Die Logistikeinrichtungen 18 synchronisieren beim Verschlüsseln oder Entschlüsseln einer Nachricht auch die Schlüssel bei Sender und Empfänger oder Teile dieser Schlüssel und sorgen dafür, daß zur Verschlüsselung nur die bisher unbenutzten Teile des Zufallsschlüssels auf den Schlüsselträgern 12 verwendet werden. Dies geschieht zum Beispiel dadurch, daß benutzte Teile eines Schlüssels gelöscht, unbrauchbar gemacht werden, oder daß die Stelle auf dem Datenträger, bis zu der hin der Schlüssel verwendet worden ist, gespeichert wird.

Das Verschlüsseln einer zu übermittelnden binären Nachricht erfolgt beispielsweise einfach dadurch, daß der Schlüssel im Binärcode zur Nachricht addiert (modulo 2) und die entstehende Zufallssequenz anschließend von einer zugeordneten Übertragungseinrichtung 20 über eine Übertragungsleitung 22 zu dem jeweiligen Empfänger übertragen wird. Von ankommenden verschlüsselten Nachrichten wird der Zufallsschlüssel wieder subtrahiert und dadurch die Nachricht entschlüsselt. Anschließend kann die Nachricht dem Telefon, Faxgerät usw. des jeweiligen Empfängers zugeführt werden. Ist ein Schlüssel ganz abgearbeitet, so kann an jedem Schlüsselgenerator 10 ein neuer, mit keinem anderen Schlüssel übereinstimmender Schlüssel bezogen werden, der dann auch wiederum nur einmal verwendet wird.

Die Leseeinrichtung 14 und die Logistikeinreichtung 18 lassen sich sehr klein und leicht ausführen, so daß sie jeweils für sich oder aber auch in einer kombinierten Einrichtung sogar in tragbare Handapparate integriert werden können, was den Anwendungsbereich des erfindungsgemäßen Verfahrens enorm erweitert.

Bei Wechselgesprächen über das Telefon muß die

Verschlüsselung und Übertragung sowie die Entschlüsselung während des Gesprächs und in den Gesprächspausen erfolgen, so daß unter Umständen Zwischenspeicher erforderlich sind, um Nachrichtenteile vor der Übertragung zu sammeln. Diese einzelnen Bauteile sind aber auch schon für normale Übertragungen und Verschlüsselungen sowie für das Lesen und Aufzeichnen von Nachrichten erforderlich.

Wenn ein Sender von Nachrichten mit mehreren Empfängern abhörsicher korrespondieren möchte, kann er für jede dieser Verbindungen einen eigenen Schlüssel verwenden, der wiederum jeweils auf zwei identischen Datenträgern 12 aufgezeichnet ist, von denen Sender und Empfänger jeweils einen bekommen. Um hier Ordnung zu halten, können die verschiedenen Datenträger 12 mit den Schlüsseln in eine Vorrichtung eingelegt werden, die die einzelnen Schlüssel den ausgewählten Empfängern zuordnet. Sie umfaßt eine Aufnahmeeinrichtung für die verschiedenen Schlüsselträger 12 und wählt beim Aufbau einer Verbindung automatisch den richtigen aus, der den selben Schlüssel enthält, den der ausgewählte Empfänger bekommen hat. Sind die Schlüsselträger CDs, so ähnelt die Vorrichtung einem Plattenwechsler in einer Musikbox. Die Zuordnung der einzelnen Schlüssel kann hierbei entweder manuell durch den Benutzer erfolgen oder aber durch eine Logistikeinrichtung der Vorrichtung selbst, die vor dem Aufbau einer Verbindung mit der Gegenlogistikeinrichtung eines Empfängers in Kontakt tritt, den eingelegten Schlüsselträger bzw. Schlüssel überprüft und automatisch den dazu passenden Schlüsselträger bzw. Schlüssel auswählt. Das Einlesen der Schlüssel von den Schlüsselträgern 12 erfolgt auch hierbei wiederum mittels einer integrierten Leseeinrichtung.

Denkbar ist auch, daß sowohl Empfänger als auch Sender über eine entsprechende Vorrichtung verfügen, in die jeweils mehrere Datenträger 12 mit Schlüsseln eingelegt werden, um dann entweder in einer fest vorgegebenen Reihenfolge

nacheinander abgearbeitet zu werden oder aber in einer von der Logistikeinrichtung des Senders bestimmten zufälligen Reihenfolge, die dann mit der Gegenlogistikeinrichtung des Empfängers in Kontakt tritt, um dort das Einlegen eines Datenträgers mit dem gleichen Schlüssel zu initiieren.

Da die zufälligen Schlüssel bei dem erfindungsgemäßen Verfahren nur auf den Schlüsselträgern 12 aufgezeichnet werden und auch den Übertragungs- und Leseeinrichtungen 20 bzw. 14 nicht bekannt werden und zudem auch nur einmal zum Verschlüsseln einer Nachricht verwendet werden, ist das Verfahren von einem unbefugten Dritten selbst mit großem Rechenaufwand und dem Einsatz modernster Entschlüsselungsverfahren praktisch nicht zu brechen solange die Schlüsselträger 14 mit den Schlüsseln nicht in unbefugte Hände gelangen, was durch entsprechende Vorsichtsmaßnahmen relativ einfach zu verhindern ist.

Patentansprüche

1. Verfahren zur gesicherten Übertragung von Nachrichten zwischen zumindest zwei Benutzern eines Telekommunikationsnetzes mit folgenden Verfahrensschritten:
   a) Erzeugung eines geheimen, zufälligen binären Schlüssels großer Länge durch einen Schlüsselgenerator (10);
   b) Einschreiben dieses Schlüssels in zumindest zwei transportable Datenträger (12) und Ausgabe dieser Datenträger (12) durch den Schlüsselgenerator (10), wobei die Benutzer je einen Datenträger (12) mit dem Schlüssel erhalten;
   c) Eingabe dieser Datenträger (12) in Leseeinrichtungen (14), die den von den Benutzern zur Nachrichtenübermittlung verwendeten Telekommunikationsendeinrichtungen (16) jeweils zugeordnet sind, und Einlesen des in die Datenträger (12) eingeschriebenen Schlüssels durch die Leseeinrichtungen (14);
   d) Aufbauen einer Verbindung zwischen den von den Benutzern zur Nachrichtenübermittlung verwendeten Telekommunikations-Endeinrichtungen (16);
   e) Überprüfen der Eingabe der Datenträger und Vergleichen der eingelesenen Schlüssel durch Logistikeinrichtungen (18), die den von den Benutzern zur Nachrichtenübermittlung verwendeten Telekommunikationsendeinrichtungen (16) jeweils zugeordnet sind; und
   f) Verschlüsseln der zu übermittelnden Nchrichten mit wenigstens einem Teil des Schlüssels bei Übereinstimmung der Schlüssel.

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet, daß nach dem Verfahrensschritt e) folgender Schritt ausgeführt wird:
- Synchronisieren der eingelesenen Schlüssel oder Teile dieser Schlüssel durch die Logistikeinrichtungen (18) zur Ver- und Entschlüsselung der zu übermittelnden bzw. empfangenen Nachrichten.

3. Verfahren nach Anspruch 1 oder 2,
dadurch gekennzeichnet,
daß von einem Benutzer i, der mit mehreren anderen Benutzern kommunizieren möchte, mehrere Datenträger (12) mit unterschiedlichen Schlüsseln ij, die jeweils einer Verbindung zwischen dem Benutzer i und einem anderen Benutzer j zugeordnet sind, in die der Telekommunikationsendeinrichtung (16) des Benutzers i zugeordnete Leseeinrichtung (14) oder eine dieser zugeordneten Einrichtung eingegeben werden, die beim Aufbau einer Verbindung zwischen den Benutzern i und j automatisch den jeweils zugeordneten Schlüssel ij auswählt und zur Verschlüsselung verwendet.

4. Verfahren nach einem der Ansprüche 1 bis 3,
dadurch gekennzeichnet,
daß ein optischer Zufallsgenerator mit Strahlteiler zur Schlüsselerzeugung verwendet wird.

5. Verfahren nach einem der Ansprüche 1 bis 3,
dadurch gekennzeichnet,
daß die spontane Emission eines Photons in elektrisch oder optisch angeregter Materie zur Schlüsselerzeugung verwendet wird.

6. Verfahren nach einem der Ansprüche 1 bis 3,
dadurch gekennzeichnet,
daß ein physikalisches Rauschverfahren oder der radioaktive Zerfall zur Schlüsselerzeugung verwendet

wird.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß der erzeugte Schlüssel nur auf den ausgegebenen Datenträgern (12) gespeichert wird.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß als Datenträger (12) ein Magnetband, eine CD oder ein geeigneter Halbleiterspeicher verwendet wird.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, daß die Anzahl und/oder die Art der Datenträger (12) frei wählbar ist.

10. Verfahren nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, daß der Schlüsselgenerator (10) öffentlich zugänglich ist.

11. Verfahren nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, daß der Schlüsselgenerator (10) durch Eingeben eines Zahlungsmittels oder einer Magnetstreifenkarte aktiviert wird.

12. Verfahren nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, daß der Schlüssel oder Teile des Schlüssels nur einmal verwendet werden.

13. Verschlüsselungssystem zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 12, gekennzeichnet durch
- wenigstens einen Schlüsselgenerator (10) mit einer

Einrichtung zum Erzeugen eines zufälligen binären Schlüssels großer Länge, einer Einrichtung zum Einschreiben des erzeugten Schlüssels in zumindest zwei transportable Datenträger (12) und einer Einrichtung zum Ausgeben der beschriebenen Datenträger (12);

- zumindest zwei Leseeinrichtungen (14) zum Einlesen des Schlüssels von den beschriebenen Datenträgern (12), die den von den Benutzern zur Nachrichtenübermittlung verwendeten Telekommunikationsendeinrichtungen (16) jeweils zugeordnet sind;
- zumindest zwei Logistikeinrichtungen (18) zur Überprüfung der Eingabe der Datenträger und zum Vergleichen der eingelesenen Schlüssel, wobei die Logistikeinrichtungen (18) den von den Benutzern zur Nachrichtenübermittlung verwendeten Telekommunikationsendeinrichtungen (16) jeweils zugeordnet sind; und
- zumindest zwei Verschlüsselungs- und/oder Entschlüsselungseinrichtungen zur Ver-und/oder Entschlüsselung von zu übermittelnden bzw. empfangenen Nachrichten mit wenigstens einem Teil der eingelesenen Schlüssel bei übereinstimmenden Schlüsseln, wobei die Ver- und/oder Entschlüsselungseinrichtungen den von den Benutzern zur Nachrichtenübermittlung verwendeten Telekommunikationsendeinrichtungen (16) jeweils zugeordnet sind.

14. Verschlüsselungssystem nach Anspruch 13, dadurch gekennzeichnet, daß die Logistikeinrichtungen zur Synchronisation der eingegebenen Schlüssel oder Teile dieser Schlüssel untereinander ausgebildet sind.

15. Verschlüsselungssystem nach Anspruch 13 oder 14,

Zusammenfassung:

Es wird ein Verfahren zur gesicherten Übertragung von Nachrichten zwischen zumindest zwei Benutzern eines Telekommunikationsnetzes mittels eines geheimen, zufälligen binären Schlüssels großer Länge beschrieben, der nur ein einziges Mal zur Verschlüsselung verwendet wird. Dieser Schlüssel wird in einem vorzugsweise öffentlich zugänglichen Schlüsselgenerator (10) beispielsweise mittels eines optischen Zufallsgenerators mit Strahlteiler erzeugt, in zumindest zwei transportable Datenträger (12), wie z.B. CDs, eingeschrieben und in dieser Form anschließend an die Benuzter ausgegeben, die jeweils einen Datenträger (12) mit dem eingeschriebenen Schlüssel erhalten. Eine weitere Speicherung des Schlüssels erfolgt nicht. Die Benutzer geben diese Schlüsselträger (12) nun in Leseeinrichtungen (14) ein, die den von ihnen verwendeten Telekommunikationsendeinrichtungen (16), wie z.B. Telefone, Faxgeräte oder PCs, jeweils zugeordnet sind. Beim Aufbau einer Verbindung wird die ordnungsgemäße Eingabe der Schlüssel und ihre Übereinstimmung durch Logistikeinrichtungen (18) überprüft, die den Telekommunikationsendeinrichtungen (16) jeweils ebenfalls zugeordnet sind und beim Verschlüsseln und Entschlüsseln der zu übermittelnden Informationen für eine Synchronisation der eingegebenen Schlüssel oder zumindest von Teilen der Schlüssel sorgen. Es wird auch ein System zur Durchführung dieses Verfahrens mit den hierfür erforderlichen Einrichtungen beschrieben.

(Fig. 1)

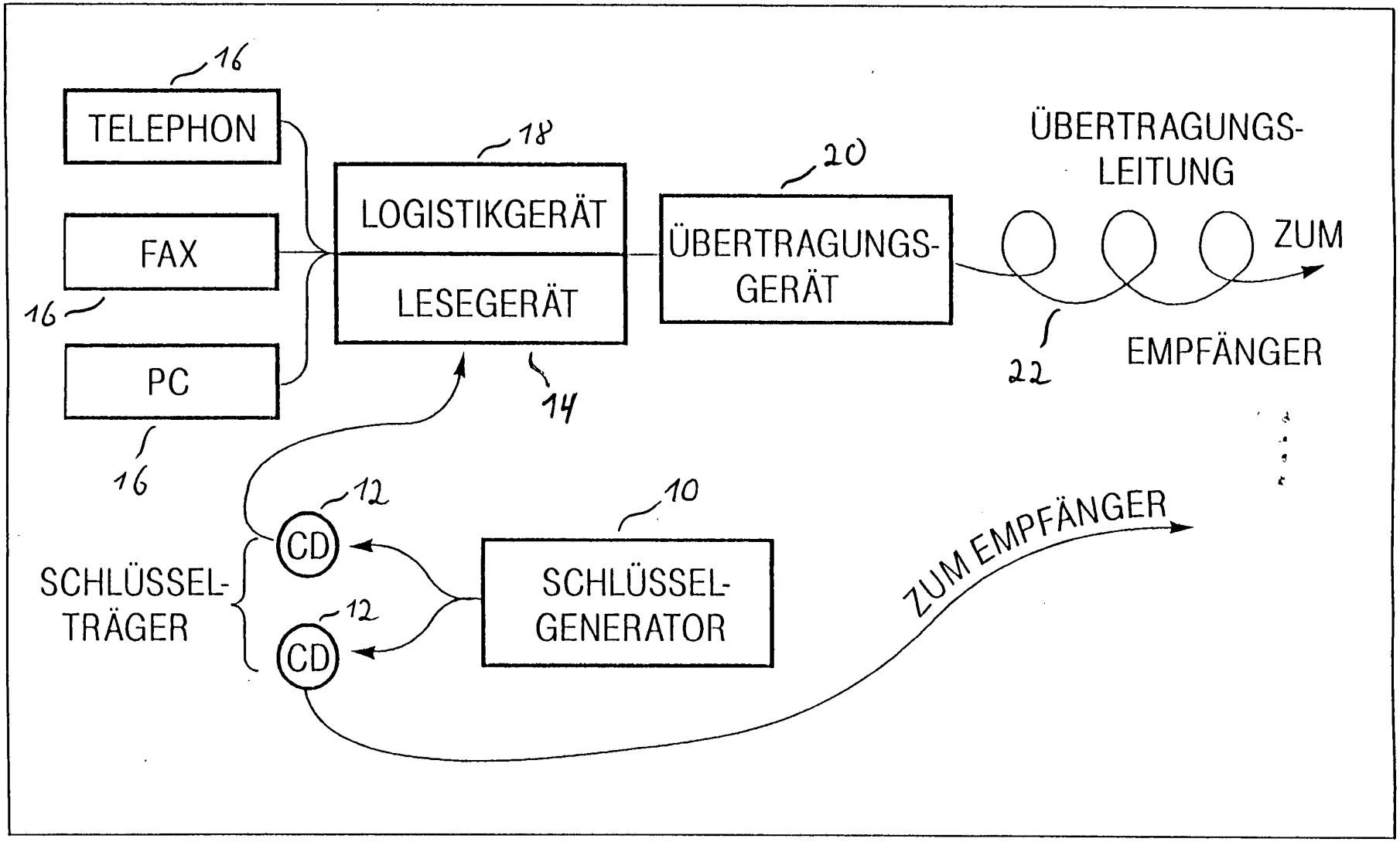
16
TELEPHON
FAX
16
PC
16
18
LOGISTIKGERÄT
LESEGERÄT
14
20
ÜBERTRAGUNGS-
GERÄT
ÜBERTRAGUNGS-
LEITUNG
ZUM
EMPFÄNGER
22
12
CD
12
CD
SCHLÜSSEL-
TRÄGER
10
SCHLÜSSEL-
GENERATOR
ZUM EMPFÄNGER

Fig. 1

US 0931590103P1

Creation date: 07-10-2004
Indexing Officer: ATHUYA - AUNG THUYA
Team: OIPEBackFileIndexing
Dossier: 09315901

Legal Date: 06-11-1999

No.	Doccode	Number of pages
1	CTMS	1

Total number of pages: 1

Remarks:

Order of re-scan issued on .....